09-20-00 A

JC872 U.S. PTO
09/19/00

JC564 U.S. PTO
09/665018
09/19/00

09665018 . 091500

UTILITY PATENT APPLICATION TRANSMITTAL *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	*Title of Invention*	Vulnerability Assessment and Authentication of a Computer by a Local Scanner
	Named Inventor(s)	Patrick Taylor, Scott Mewett, Phillip C. Brass, Theodore R. Doty
	Attorney Docket	05456.105007
	Express Mail Label No.	EF045414342US

APPLICATION ELEMENTS

1. □ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification, Claims, and Abstract — Total Pages **17**
3. ☒ Drawings — Total Sheets **3**
4. Oath or Declaration — Total Pages **4**
a. ☒ Unexecuted
b. □ Copy from prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 Below]
(i) □ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. □ Incorporation by Reference
(usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. □ Microfiche Computer Program *(Appendix)*
7. □ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
a. □ Computer Readable Copy
b. □ Paper Copy (identical to computer copy)
c. □ Statement verifying identity of above copies

ADDRESS TO:
Assistant Commissioner of Patents
Box Patent Application
Washington, D.C. 20231

ACCOMPANYING APPLICATION PARTS

8. □ Assignment Papers (cover sheet & document(s))
9. □ 37 CFR 3.73(b) Statement
(when there is an assignee)
□ Power of Attorney by assignee
10. □ English Translation Document *(if applicable)*
11. □ Information Disclosure Statement (IDS) PTO-1449
□ Copies of IDS Citations
12. □ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. □ Small Entity Statement(s)
□ Statement filed in prior application Status still proper and desired
15. □ Certified Copy of Priority Document(s)
16. □ Other: ____________________

17. If a **CONTINUING APPLICATION**, *check appropriate box and supply the requisite information*:
□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No:

18. CORRESPONDENCE ADDRESS:

W. Scott Petty, Esq.
KING & SPALDING
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303

By: ____________________ Reg. No. 35,645
Date: September 19, 2000
Telephone: 404.572.4600
Facsimile: 404.572.5145

VULNERABILITY ASSESSMENT AND AUTHENTICATION OF A COMPUTER BY A LOCAL SCANNER

RELATED APPLICATION

The present application is related to U.S. Patent Application Serial No. 09/607,375, filed on June 30, 2000, entitled "Method and Apparatus for Network Assessment and Authentication," which is fully incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to network security for distributed computer systems and, more specifically, to granting computer services based upon a local vulnerability assessment of a computer by a browser-based scanner operating on that computer.

BACKGROUND OF THE INVENTION

While the open network architecture of the Internet permits a user on a network to have access to information on many different computers, it also provides access to messages generated by a user's computer and to the resources of the user's computer. In fact, there are persons who attempt to use knowledge regarding the operations of the protocol stack and operating systems in an effort to gain access to computers without authorization. These persons are typically called "hackers." hackers present a significant security risk to any computer coupled to a network where a user for one computer may attempt to gain unauthorized access to resources on another computer of the network. For example, an employee may attempt to gain access to private and confidential employee records on a computer used by the human resources department of an employer.

The present invention solves the security compromise problem by using services provided by a scanner operable with a Web-enabled browser for the invocation and execution of scans and risk assessment. The invention can accomplish this desirable objective using a browser-based tool to scan the user's workstation for evidence of a security compromise or a vulnerability.

09665018 .091900

SUMMARY OF THE INVENTION

The disadvantages of the prior art are overcome by the present invention, which can complete a local scan of a workstation upon installation of a browser-based scanner provided to the workstation by a remote server via a distributed computer network. A remote server receives a request for an on-line scanner from a browser operating on a workstation connected to a computer network. In response to receiving the scanner via the network, the browser installs the scanner at the workstation to support the completion of vulnerability assessment scans within the local operating environment of the workstation. Using this local scanner, the browser can perform a scan of the workstation and its operating environment and generate a scan results report for presentation to the user or a system administrator. The browser also can transmit the scan results to the remote server for archival storage and subsequent reporting. In one aspect of the invention, the browser can attempt to address an identified security risk by implementing a repair solution or "fix of the workstation."

In view of the foregoing, it will be understood that the present invention can deploy a scanning tool from a remote server to a browser-enabled workstation to support a local assessment of the vulnerability of a workstation coupled to a computer network. This scanning tool can operate within the browser environment to complete a scan of the workstation and to generate workstation credentials. The advantages and implementation of the present invention will be described in more detail below in connection with the detailed description, the drawing set, and the attached claims.

09695018.050100

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating the primary components of a network security system, including a local workstation assessment service on a workstation, in accordance with an exemplary embodiment of the present invention.

Figure 2 is a diagram showing interactions between a browser and a Web server in a Web-based security system in accordance with an exemplary embodiment of the present invention.

Figure 3 is a diagram illustrating interactions between a browser and a Web server in a Web-based security system using a scanner operating within a browser environment on a workstation in accordance with an alternative exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

In environments where computers are shared, users want an assurance that the computer they are accessing is secure, before completion of the log-in operation. For an exemplary embodiment, a local scanner can complete a vulnerability assessment of the workstation and provide the scan results to the user or to a system administrator. If the local scanner finds a vulnerability, a local process can inform the user that the machine is or may be compromised, or repair an identified vulnerability. The local scanner can be implemented as a plug-in or a control for operation with a browser operating on the workstation. For example, the local scanner can be implemented as an ActiveX control maintained at a Web server available for download to a workstation in response to a network request transmitted by a browser operated on the workstation. Once installed, the ActiveX control can operate in tandem with the browser to perform a vulnerability assessment of the workstation and to generate a report identifying the scanned results.

For another exemplary embodiment, the results of the local host assessment can be provided to a network server prior to the delivery of the requested network service to the workstation. For example, a local scanner operating in tandem with a browser on the workstation can complete a vulnerability assessment of the workstation and supply the scan results to the browser installed on workstation. In turn, the browser can transmit the local scan results to the network server via the computer network for evaluation by the network server. Performing a vulnerability assessment at the local level of the workstation allows a network server to determine whether the workstation is a "trusted" platform from which to accept network service requests. If the vulnerability assessment shows that the computer is compromised, or if the possibility of remote compromise is high, the network server can deny service to the workstation. Optionally, the network server can distribute a vulnerability assessment tool via the computer network to repair the vulnerability of the workstation.

Turning now to the drawing set, in which like numbers reference like elements, Fig. 1 illustrates a client-invoked vulnerability assessment of a workstation in which the workstation credentials are generated locally at the workstation. In other words, the vulnerability assessment is invoked at the client and the assessment is completed by a local workstation assessment service on the workstation. Workstation credentials typically include information about the current integrity of the workstation and the security posture of the workstation. For example, security posture can include data that indicates the potential for the workstation to be compromised by an unauthorized user or service. As shown in Fig. 1, an exemplary network security system 100 comprises a workstation 115 operating a local workstation assessment service in a network environment including a distributed computer network 125 and a network server 120. A client application 130 retrieves workstation credentials, typically including workstation integrity information and workstation security posture information, from the local workstation assessment service 135 on the workstation 115. The local workstation assessment service 135 generates the workstation credentials by completing a local vulnerability examination of the workstation 115.

The client application 130 can present the results of the local scan assessment, namely the workstation credentials, to the user. This allows the user to compare the scan assessment results to a workstation security policy to determine the extent to which the workstation 115 complies with that security policy. In the event that the local workstation assessment service 115 detects a vulnerability, the client application 130 can present to the user the recommended course of action to repair the detected vulnerability. The client application 130 can be implemented by a browser, such as the "INTERNET EXPLORER" browser marketed by Microsoft Corporation, and the local workstation assessment service 135 can be implemented by a scanner plug-in or control for installation at the browser. For example, the local workstation assessment service 135 can be embodied by an ActiveX control available for download from the Web server for use with the browser operating on the workstation 115 to complete local scan operations. The plug-in or control operates in tandem with the browser to complete a scan of the workstation and its environment and to generate scan results.

The client application 130, which also resides on the workstation 115, can present the local scan results to a network service 140 on the network server 120. The network service 140 can store the local scan results of the server 120 to create an archival record of the vulnerability assessment of the workstation 115. The network service 140 can also decide whether to provide service to the workstation 115 via the network 125 based on workstation credentials, namely the local scan results. Specifically, the network service 140 completes this decision-making process by evaluating the workstation against a workstation security policy. This allows the network service 140 to determine the extent to which the workstation 115 complies with its security policy. The network service 140 typically uses a policy compliance measurement to decide what, if any, service level to be the supplied to the workstation 115. In the alternative, the network service 140 can transmit a vulnerability assessment tool to repair the vulnerability of the workstation 115.

An exemplary process 200 for a Web-based authentication service relying upon browser-based technology is shown in Fig. 2. Turning to Fig. 2, the process 200 is initiated by a browser 205, operating on a workstation coupled to a computer network. The browser 205 issues a request to a network server, such as a Web server 210, via a distributed computer network, such as the Internet or a corporate intranet. Responsive to the request, the Web server 210 transmits a workstation assessment agent, which may be a "JAVA" applet, ActiveX control, browser plug-in, or other Web-based executable content, to the Web browser 205 in response to the request. Once installed at the browser 205, the workstation assessment agent generates workstation credentials based on a local examination of the workstation. For example, if the workstation assessment agent is implemented as a browser plug-in, also described as an authentication plug-in, the plug-in operates within the browser environment to complete a scan of the host computer. The results of this vulnerability scan represent workstation credentials. For the representative example shown in Fig. 2, the workstation assessment agent is implemented by a browser plug-in 205'.

The workstation assessment agent, i.e., the browser plug-in 205', transmits the workstation credentials to the Web server 210 via the computer network. An application on the Web server 210, typically a CGI 215, compares the workstation credentials to a workstation security policy to decide whether the workstation is secure. Service by the Web server 210 is allowed if the CGI 215 determines that the workstation is secure and the Web server 210 authenticates the user. If the CGI 215 decides to continue, and the Web server 210 has not already authenticated the user, the server may begin the user authentication process. There is a benefit to authenticating the user after completing a vulnerability analysis of the workstation – it is more difficult for an intruder to steal a user's credentials if the intrusion is detected and the user authentication process is terminated before the user presents their credentials.

Table I provides an overview of the primary network service authentication tasks completed for the Web-based operating environment of a workstation assessment agent operating on a workstation and a Web server, as shown in Fig. 2. The workstation assessment agent completes vulnerability assessment tasks

09595018.061500

and transmits the assessment results to the Web server. In turn, the Web server determines whether to provide a network service to the workstation based on the assessment results.

Table I

1. The user of a workstation requests a log-in page from a Web server, typically by clicking a button or link on a Web page to begin the authentication process.

2. A browser, operating at the workstation, loads a log-in page or a host authentication page from the Web server. The host authentication page typically contains a browser plug-in representing a workstation assessment agent.

3. The browser plug-in performs a host assessment scan of the workstation.

4. The browser plug-in sends the scan results from the browser via a secure link to a CGI script on the Web server.

5. The CGI script uses the scan results to decide whether to grant the workstation access to a network service at the Web server.

6. If the workstation is granted access, the CGI script redirects the browser to the next step in the authentication process, namely user authentication. If the workstation is denied access, the CGI script redirects the browser to a page that explains to the user why the workstation cannot be granted access to the Web server. This page also describes what the user can do to bring the host into compliance so that access will be granted.

The exemplary Web-based process shown in Fig. 2 is supported by two separate components: (1) the browser plug-in 205' that performs the workstation assessment in connection with browser operations; and (2) the CGI script 215, which evaluates the workstation credentials generated by the asessment and determines whether the host satisfies authentication requirements. The browser plug-in and the

CGI script are representative embodiments of software routines that operate on the workstation and the Web server, respectively. The workstation assessment service is provided by the browser plug-in and implemented by a variety of different software routines, including a Java applet or an ActiveX control. Likewise, the network service implemented by the CGI script can be implemented by other conventional Web-based executable software programs. Consequently, it will be understood that the present invention is not limited to a particular Web-based implementation, such as the representative exemplary embodiment illustrated in Fig. 2.

The workstation assessment agent, implemented as a browser plug-in 205', has three main functions: host assessment; communication of workstation assessment results; and reporting workstation assessment results. The host assessment is completed to determine whether the workstation is compromised. The browser plug-in 205' runs a series of checks or exploits, each looking for a particular security risk. Each check generates a scan result, which indicates whether a vulnerability risk is present at the workstation. The browser plug-in 205' then prepares assessment results for transmission to the Web server.

The browser plug-in 205' communicates the assessment results to the CGI script 215 operating on the Web server 210. This communication is preferably completed in a secure manner, between the workstation and the Web server, so that results cannot be intercepted by a third party. The communication also should be secure in such a way as to prevent the transmission of false information to the CGI script 215. This can be accomplished by the use of authentication or encryption technologies

For example, the communication between the browser plug-in 205' and the CGI script 215 can be completed by sending an HTTPS GET request with vulnerability assessment results stored as parameters of the GET request. The browser plug-in 205' can generate a URL that uses HTTPS for confidentiality and contains the scan results as parameters. These parameters can be obfuscated by using shared secret encryption to prevent reverse engineering of the communications channel and to insure transmission only to appropriate servers.

The CGI script 215 receives scan results from a Web-enabled client and decides, based on the results, whether to continue the authentication process. The script 215 responds to the scan results by redirecting the Web client, i.e., the workstation, to one of two different Web pages based on this decision. If the script 215 decides to allow authentication to continue, it redirects the browser 205 to a page that continues or completes the log-on process. If the script 215 decides to deny access, it redirects the browser 205 to a page that explains that service is denied, why access is denied, and what can be done to obtain access to the requested service.

The CGI script 215 is preferably capable of receiving encrypted data comprising scan results from the browser plug-in 205', decrypting the data, and making a decision based on the results. The script 215 can assign a score to each different vulnerability identified by the browser plug-in 205'. When all results are received from the browser plug-in 205', the script 215 calculates a total score by adding the score assigned to each vulnerability. The total score is then compared by the script 215 against a maximum allowable score. If the total score is less than or equal to the maximum allowable score, authentication is allowed to proceed. If the total score is greater than the maximum allowable score, access by the workstation to the Web server 210 is denied by the script 215.

The Web-based design illustrated in Fig. 2 requires the server to decide, based on security assessment information from the client, whether or not to grant access, or to possibly grant restricted access to a client workstation. In the alternative, the client can make that decision, given sufficient decision-making information at the workstation or received from the server. For example, a browser operating on a workstation can issue a request for a log-in page to a network server. In response, the network server can transmit the log-in page, an authentication plug-in, and a workstation policy to the workstation via the computer network. The authentication plug-in is installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network. The workstation security credentials can be compared to the workstation policy on the workstation to determine whether the workstation should be granted access to a software service of the network.

In many web service contexts, the result of a decision-making process for determining whether to grant access by a client to a network service can be expressed as making a choice between URLs. If the decision comes out one way, the browser points to one URL. If it comes out another way, the browser points to a different URL. This can be accomplished on the server side by instructing the client to submit scan information to the server, and having the server redirect the client to the appropriate URL after making the service access decision.

In the past, a local host scanning device has typically been implemented as an installable, executable program that uses services provided by the operating system on a workstation for the completion of vulnerability assessment scans. In contrast to the prior art, the present invention operates within the environment of a browser on a workstation to complete vulnerability assessments of the workstation and its operating environment. In an alternative exemplary embodiment, a browser operating on the workstation can request a scanner from a Web server via a computer network. The Web server transmits the scanner to the browser via the computer network for installation at the local workstation, otherwise described as a client computer. The scanner is a browser-based program that can be downloaded from a remote server to a browser-compatible workstation to complete local vulnerability assessments without the use of operating system services. Upon installation at the browser, the scanner can complete vulnerability assessment operations and generate a report describing the scan results. The scan results can be presented to the user or to a system administrator responsible for resources of the computer network coupled to the workstation. The scanner also can attempt to repair an identified security risk. Vulnerability assessments and repair operations are completed within the Web-enabled browser environment.

Turning now to Fig. 3, an exemplary browser-enabled operating environment 300 comprises a workstation with a Web-compatible browser 305 and a Web server 310, each coupled to a computer network (not shown), such as the global Internet or a corporate intranet. To initiate installation of a scanner, the browser 305 transmits a request via the computer network to a network server, such as the Web server 310. The Web server 310 typically publishes a Web page that hosts the scanner for download to a requesting workstation. For an exemplary embodiment, the scanner is packaged as an ActiveX control for operation within an ActiveX-compatible browser, such as Microsoft's "INTERNET EXPLORER" browser program. For example, the scanner can comprise an ActiveX control DLL and a data file comprising vulnerability descriptions, both packaged within a .CAB file. Alternative embodiments of the scanner can include a JAVA applet, a browser plug-in, or another Web-based executable tool.

The browser 305 can download the scanner by accessing an OBJECT tag at the control hosting page published by the Web server 310. The OBJECT tag typically comprises a class identifier (ID) for an ActiveX control and a uniform resource locator (URL) to the online scanner program (.CAB file) containing the

ActiveX control. The scanner program typically includes a current version identifier for the ActiveX control. The browser 305 preferably uses the current version of the ActiveX control to support online scan operations within the browser environment of the workstation. If an ActiveX control with the specified class ID has been installed at the workstation, the browser can compare the version number for that ActiveX control to the version number specified by the OBJECT tag. If the version number in the OBJECT tag represents a more recent version of the ActiveX control, then the browser can download the current version of the ActiveX control to deploy the online scanner. If, on the other hand, the version number for the currently installed ActiveX control is the same as or less than the OBJECT tag, then the browser should not download a new copy of the ActiveX control. This functionality is supported by Microsoft's "INTERNET EXPLORER" browser and is used by the exemplary embodiment to operate an online scanner within the browser environment of the workstation based upon the current version of the appropriate ActiveX control.

In response to the deployment request, the control hosting page at the Web server 310 transmits the online scanner to the browser 305 at the workstation via the computer network. Upon completing the download operation, the browser 305 can use "Authenticode" technology to verify the identity of the publisher of the ActiveX control for the scanner and to query the user whether the scanner should be installed as part of the browser operating on the workstation. As known to those of skill in the art, Authenticode technology comprises a special signing key and the signing of either the ActiveX control or the .CAB file representing the scanner. This signing key must, in turn, be signed by a trusted third party to support a secure installation of the scanner at the browser 305. For example, Verisign can provide a code-signing key to sign the ActiveX control of the scanner program. Upon downloading the scanner, the browser 305 can query the user as to whether the user wishes to download an ActiveX control published by a publisher having an identity verified by Verisign.

Upon completion of the installation operation, the browser-compatible scanner 305' can complete vulnerability assessments of the local workstation and its operating environment. The scanner 305' can generate a report in response to completing vulnerability assessment scan operations. The scanner 305' typically presents this report to the user or to a system administrator for the computer network coupled to the workstation. For example, the scanner 305' can display the scan results as a report published in the form of a HYPERTEXT MARKUP LANGUAGE

09651518.090500

(HTML) page published at the workstation. The scanner also can transmit the results using the HTTP or HTTPS protocol to a remote server, such as the Web server 310, for archival storage and to generate subsequent reports. The scanner 305' can support this transmission of scan results via the computer network based upon a browser-supplied application programming interface (API).

For an exemplary embodiment, the scanner 305' also can attempt to repair security risks identified by the vulnerability assessment report. In the alternative, the scanner can identify a repair solution in the report presented to the user or to the system administrator. It will be understood that an optional scanner operation is the transmission of scan results via the browser 305 to another server connected to the computer network.

Significantly, the present invention supports the distribution and execution of a vulnerability assessment tool within a browser operating at a workstation coupled to a computer network. Although this online scanner is typically supported by Microsoft's ActiveX control technology, it will be understood that alternative Web technologies can be used to implement the online scanner, including Sun's "JAVA" language or other Web-deployed technologies, such as "JavaScript", VBScript, and Macromedia's "Shockwave" technologies. Rather than install a software program for operation with the operating system of a workstation, the present invention can support a vulnerability assessment of the workstation and its operating environment via a Web-enabled browser. This enables the scanner to be installed on a central server for deployment to multiple workstations via a browser operating on each workstation.

In view of the foregoing, it will be understood that the present invention also provide a Web-based system for completing local scan assessments of a workstation in connection with the operation of a browser running on that workstation. The scanner can be downloaded to the workstation from a Web server and installed as a plug-in or control within the browser environment of the workstation. The scanner can complete a local scan of the workstation and its operating environment and generate workstation assessments results for presentation to the user or delivery to a network server.

The above-described embodiments are presented as illustrative examples. Although the preferred operating environment for the present invention is a Web-based computing environment, such as the Internet, those skilled in the art that the present invention is operable within other forms of distributed computer networks,

09565018.050600

such as local area or wide area network. It will be readily appreciated that deviations may be made from the specific embodiments disclosed in this specification without departing from the invention. Accordingly, the scope of this invention is to be determined by the claims below rather than being limited to the specifically described embodiments above.

09665018.091900

CLAIMS

What is claimed is:

1. A computer-implemented process for assessing the vulnerability of a workstation to a security compromise, comprising the steps:

issuing a request for a scanner from a browser operating on the workstation to a network server via a computer network;

transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to complete a vulnerability assessment of the workstation; and

generating workstation credentials in response to the scanner conducting the vulnerability assessment of the workstation.

2. The computer-implemented process of Claim 1 further comprising the step of presenting the workstation credentials to the user of the workstation.

3. The computer-implemented process of Claim 1 further comprising the step of transmitting the workstation credentials to the network server via the computer network.

4. The computer-implemented process of Claim 1 further comprising the step of completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation.

5. The computer-implemented process of Claim 1 wherein the scanner comprises a plug-in control operable with the browser and a data file defining security vulnerabilities.

09655018.091600

6. The computer-implemented process of Claim 1, wherein the step of issuing a request for a scanner comprises the browser issuing a request for a Web page at the network server, the Web page hosting the scanner as a plug-in control available for installation with the browser.

7. A computer-readable medium comprising the computer-implemented process of Claim 1.

09555018.091500

8. A computer-implemented process for authenticating a workstation requesting a software service, comprising the steps:

issuing a request for a scanner to a network server from a browser operating on the workstation;

transmitting the scanner and a workstation policy from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation;

comparing the workstation credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to the software service.

9. The computer-implemented process of Claim 8, wherein the step of issuing a request for a scanner comprises the browser issuing a request for a Web page at the network server, the Web page hosting the scanner as a control operable with the browser.

10. A computer-readable medium comprising the process of Claim 8.

09656018.091600

11. A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a scanner to the network server from a browser operating on the workstation;

transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

transmitting the workstation security credentials from the scanner to the network server via the computer network; and

determining at the network server whether the workstation should be granted access to a network service of the network based on the workstation credentials.

09659018.061600

12. The computer-implemented process recited by Claim 11 wherein the network server comprises a CGI script and the step of determining whether the workstation should be granted access to the network service comprises the CGI script comparing the workstation credentials to a workstation security policy maintained at the network server to determine whether the workstation should be granted access to the network service;

if the workstation credentials satisfy the workstation security policy, then authorizing access to the network service and directing the browser to the log-in page via the computer network,

otherwise, denying access to the network service and delivering an access denied page to the workstation via the computer network.

13. A computer-readable medium comprising the computer-implemented process of Claim 11.

14. The computer-implemented process of Claim 11, wherein the step of issuing a request for a scanner comprises the browser issuing a request for a Web page at the network server, the Web page hosting the scanner as a plug-in control available for installation with the browser.

ABSTRACT

VULNERABILITY ASSESSMENT AND AUTHENTICATION OF A COMPUTER BY A LOCAL SCANNER

Providing a user with assurance that a computer is secure based on a vulnerability assessment completed by a browser-compatible scanner operating on the computer. If the scanner finds a vulnerability, the scanner can inform the user that the machine is or may be compromised, or repair the vulnerability. For example, the scanner may be able to repair the vulnerability of the workstation. In the alternative, the scanner can provide the scan results to a network server. If the vulnerability assessment shows that the workstation is compromised, or if the possibility of remote compromise is high, the network server can decline to provide network services to the workstation.

K&S Docket No. 05456.105007

09665018.091900

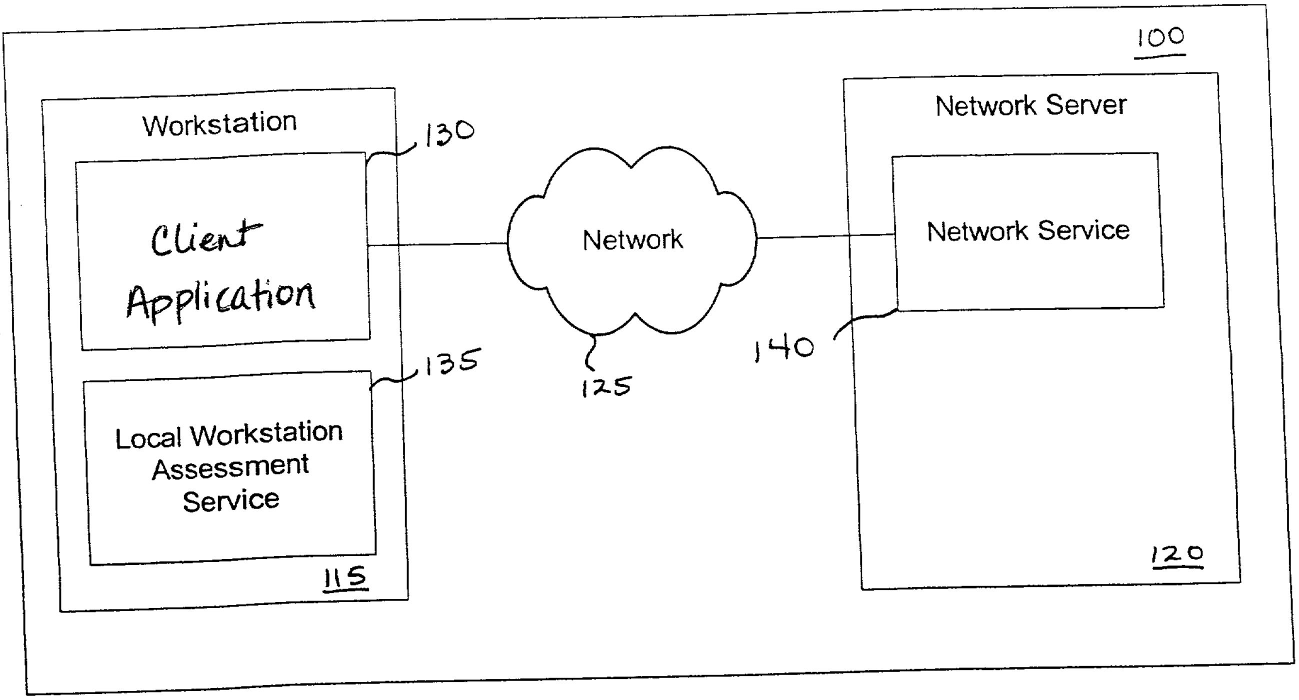
100
Workstation
130
Client Application
135
Local Workstation Assessment Service
115
Network
125
Network Server
Network Service
140
120

Figure 1

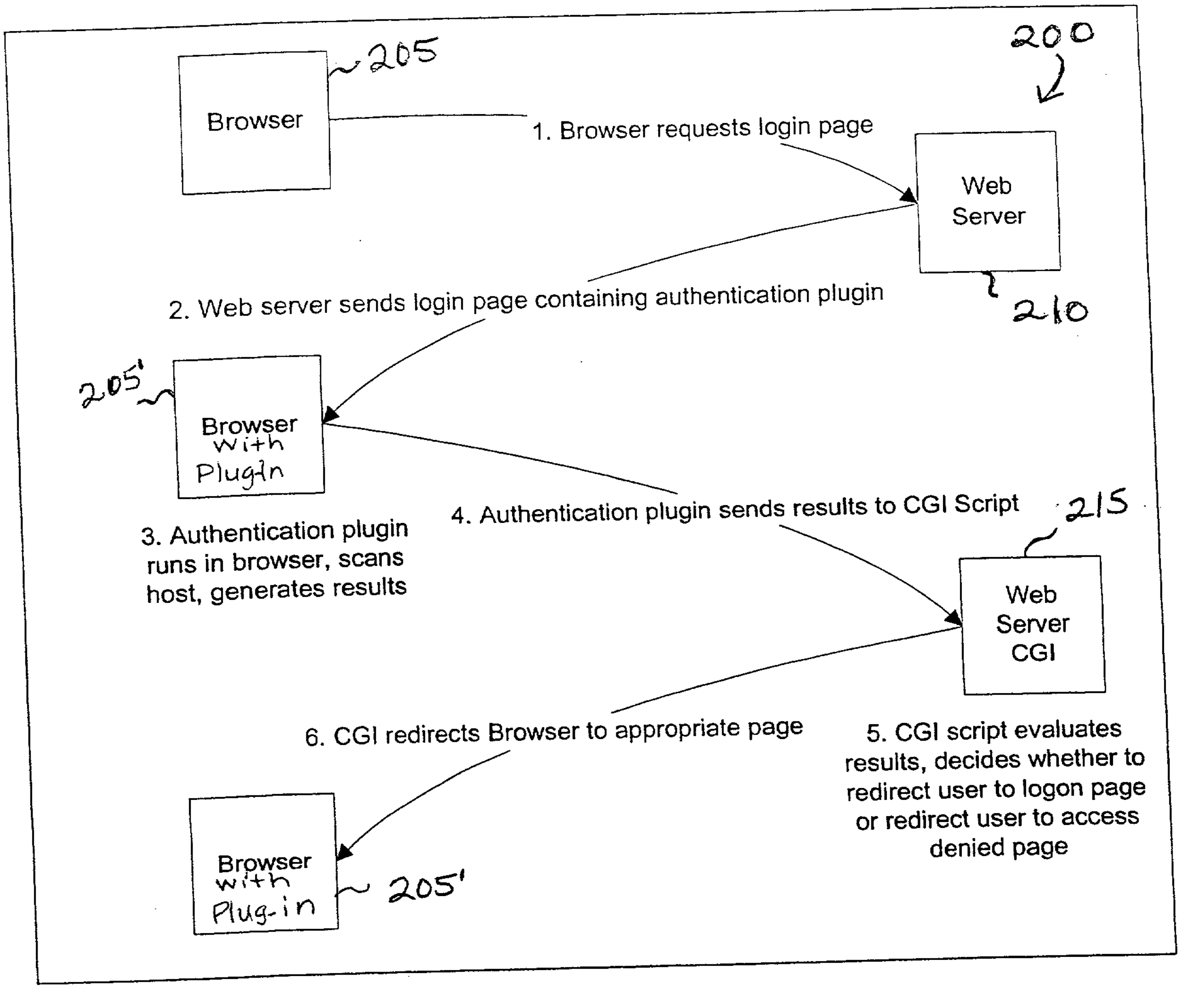
200
Browser
205
1. Browser requests login page
Web Server
210
2. Web server sends login page containing authentication plugin
205'
Browser with Plugin
3. Authentication plugin runs in browser, scans host, generates results
4. Authentication plugin sends results to CGI Script
215
Web Server CGI
5. CGI script evaluates results, decides whether to redirect user to logon page or redirect user to access denied page
6. CGI redirects Browser to appropriate page
Browser with Plug-in
205'

Figure 2

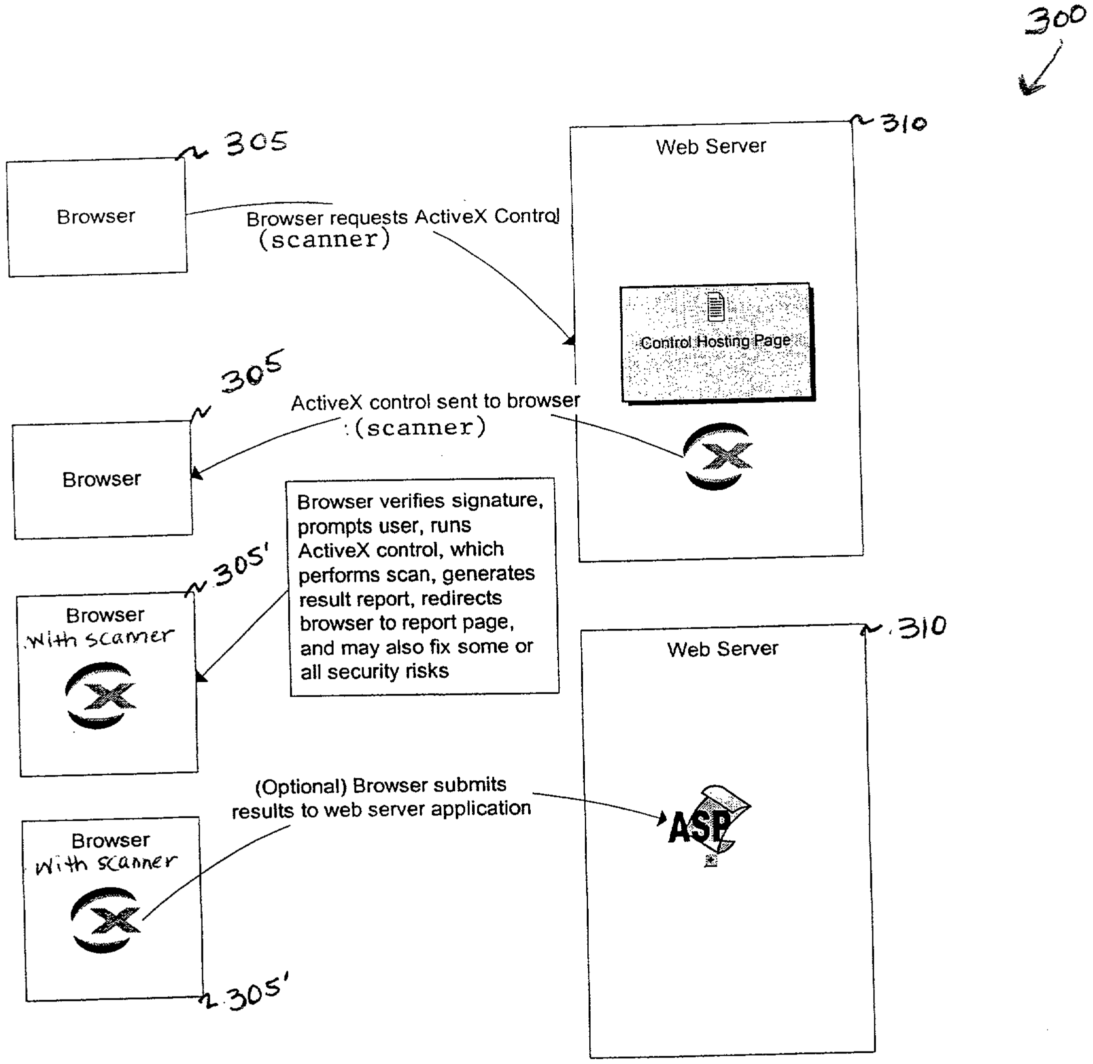
300
305
Browser
Browser requests ActiveX Control
(scanner)
310
Web Server
Control Hosting Page
305
ActiveX control sent to browser
(scanner)
Browser
305'
Browser
with scanner
Browser verifies signature, prompts user, runs ActiveX control, which performs scan, generates result report, redirects browser to report page, and may also fix some or all security risks
310
Web Server
(Optional) Browser submits results to web server application
ASP
Browser
With scanner
305'

Figure 3

DECLARATION AND POWER OF ATTORNEY Attorney's Docket No. **05456.105007**

In re Application of: **Patrick Taylor, Scott Mewett, Philip C. Brass, Theodore R. Doty**

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name. I believe I am a original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Vulnerability Assessment and Authentication of a Computer by a Local Scanner**, the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used by others in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to the date of this application. I further state that the invention was not in public use or on sale in the United States of America more than one year prior to the date of this application. *I understand that I have a duty of candor and good faith toward the Patent and Trademark Office,* and I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(d) of the foreign application(s) for patent or inventor's certificate listed below, and have also identified below any foreign application for patent or inventor's certificate disclosing subject matter in common with the above-identified specification and having a filing date before that of the application on which priority is claimed:

Application No.	Country	Filing Date	Priority Claimed Under 35 USC §119
None			Yes______ No___X___

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

None			
(Application No.)	(Filing Date)	(Application No.)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter disclosed and claimed in the present application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: patented, pending, abandoned
None		

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statement were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

POWER OF ATTORNEY: The following are hereby appointed to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Sherry M. Knowles-33,052; W. Scott Petty-35,645; Clark G. Sullivan-36,942; Steven P. Wigmore-40,447; Curtis L. Doster-41,714; Charles Vorndran-45,315; Lisa K. Norton-44,977.

Send correspondence to:
King & Spalding
191 Peachtree Street, N.E., 45th Floor
Atlanta, Georgia 30303

Direct telephone calls at **(404) 572-4600**
W. Scott Petty

Full name of first inventor: Patrick Taylor	Citizenship: U.S.
Inventor's signature	Date:
Residence and Post Office Address: 3769 Castlegate Drive, Atlanta, Georgia 30327	

09855018 . 061500

DECLARATION AND POWER OF ATTORNEY Attorney's Docket No. **05456.105007**

In re Application of: **Patrick Taylor, Scott Mewett, Philip C. Brass, Theodore R. Doty**

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name. I believe I am a original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Vulnerability Assessment and Authentication of a Computer by a Local Scanner**, the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used by others in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to the date of this application. I further state that the invention was not in public use or on sale in the United States of America more than one year prior to the date of this application. *I understand that I have a duty of candor and good faith toward the Patent and Trademark Office,* and I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(d) of the foreign application(s) for patent or inventor's certificate listed below, and have also identified below any foreign application for patent or inventor's certificate disclosing subject matter in common with the above-identified specification and having a filing date before that of the application on which priority is claimed:

Application No.	Country	Filing Date	Priority Claimed Under 35 USC §119
None			Yes______ No __X__

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

None			
(Application No.)	(Filing Date)	(Application No.)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter disclosed and claimed in the present application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: patented, pending, abandoned
None		

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statement were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

POWER OF ATTORNEY: The following are hereby appointed to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Sherry M. Knowles-33,052; W. Scott Petty-35,645; Clark G. Sullivan-36,942; Steven P. Wigmore-40,447; Curtis L. Doster-41,714; Charles Vorndran-45,315; Lisa K. Norton-44,977.

Send correspondence to:

King & Spalding
191 Peachtree Street, N.E., 45th Floor
Atlanta, Georgia 30303

Direct telephone calls at **(404) 572-4600**

W. Scott Petty

Full name of first inventor: Scott Mewett	Citizenship: Australian
Inventor's signature	Date:
Residence and Post Office Address: 88 Baronia Crescent, Holloways Beach, Cairns, Queensland, Australia	

09665018.091900

DECLARATION AND POWER OF ATTORNEY Attorney's Docket No. **05456.105007**

In re Application of: **Patrick Taylor, Scott Mewett, Philip C. Brass, Theodore R. Doty**

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name. I believe I am a original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Vulnerability Assessment and Authentication of a Computer by a Local Scanner**, the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used by others in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to the date of this application. I further state that the invention was not in public use or on sale in the United States of America more than one year prior to the date of this application. *I understand that I have a duty of candor and good faith toward the Patent and Trademark Office,* and I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(d) of the foreign application(s) for patent or inventor's certificate listed below, and have also identified below any foreign application for patent or inventor's certificate disclosing subject matter in common with the above-identified specification and having a filing date before that of the application on which priority is claimed:

Application No.	Country	Filing Date	Priority Claimed Under 35 USC §119
			Yes______ No __X__
None			

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

None			
(Application No.)	(Filing Date)	(Application No.)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter disclosed and claimed in the present application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: patented, pending, abandoned
None		

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statement were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

POWER OF ATTORNEY: The following are hereby appointed to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Sherry M. Knowles-33,052; W. Scott Petty-35,645; Clark G. Sullivan-36,942; Steven P. Wigmore-40,447; Curtis L. Doster-41,714; Charles Vorndran-45,315; Lisa K. Norton-44,977.

Send correspondence to:

King & Spalding
191 Peachtree Street, N.E., 45th Floor
Atlanta, Georgia 30303

Direct telephone calls at **(404) 572-4600**

W. Scott Petty

Full name of second inventor: Philip C. Brass	Citizenship: U.S.
Inventor's signature	Date:
Residence and Post Office Address: 1140 Pine Grove Point Drive, Roswell, Georgia 30075	

09695018.061600

DECLARATION AND POWER OF ATTORNEY Attorney's Docket No. **05456.105007**

In re Application of: **Patrick Taylor, Scott Mewett, Philip C. Brass, Theodore R. Doty**

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name. I believe I am a original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Vulnerability Assessment and Authentication of a Computer by a Local Scanner**, the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I do not know and do not believe that the same was ever known or used by others in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to the date of this application. I further state that the invention was not in public use or on sale in the United States of America more than one year prior to the date of this application. *I understand that I have a duty of candor and good faith toward the Patent and Trademark Office,* and I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(d) of the foreign application(s) for patent or inventor's certificate listed below, and have also identified below any foreign application for patent or inventor's certificate disclosing subject matter in common with the above-identified specification and having a filing date before that of the application on which priority is claimed:

Application No.	Country	Filing Date	Priority Claimed Under 35 USC §119
None			Yes______ No __X__

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

(Application No.)	(Filing Date)	(Application No.)	(Filing Date)
None			

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter disclosed and claimed in the present application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: patented, pending, abandoned
None		

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statement were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

POWER OF ATTORNEY: The following are hereby appointed to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Sherry M. Knowles-33,052; W. Scott Petty-35,645; Clark G. Sullivan-36,942; Steven P. Wigmore-40,447; Curtis L. Doster-41,714; Charles Vorndran-45,315; Lisa K. Norton-44,977.

Send correspondence to:

King & Spalding
191 Peachtree Street, N.E., 45th Floor
Atlanta, Georgia 30303

Direct telephone calls at **(404) 572-4600**

W. Scott Petty

Full name of third inventor: Theodore R. Doty	Citizenship: U.S.
Inventor's signature	Date:
Residence and Post Office Address: 540 Summerhill Drive, Roswell, Georgia 30075	